LANSCOPE
Endpoint Manager

新たな時代に向けた学びの環境

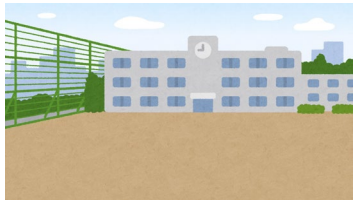
教育情報セキュリティポリシーに関するガイドラインを解説

文部科学省は2015年から教育現場のIT化を推進！教育現場が大きく変わろうとしています

少子化が進む教育現場の効率化にIT化は欠かせません。教育現場のICT化のための取り組みが進んでいます

教育機関のICT化促進

＜課題＞
- 少子化
- 子供のIT対応力向上
- 教員の多忙



GIGAスクール構想

- 生徒1人に1台のPCを配布
- 教育現場に大容量の通信ネットワークの整備
- 教育データの標準化（データの利活用）
- 最先端技術活用促進

新学習指導要綱

- プログラミング授業の必須
- デジタル教科書／教材

教育現場の働き方改革

- 部活動の地域シフト
- 教師の勤務時間見直し

学校における働き方改革推進本部設立

2017

- 教育ICTガイドブック

2019

- 地方公共団体における情報セキュリティポリシーに関するガイドライン
- 教育情報セキュリティポリシーに関するガイドライン
- 新学習指導要綱（小→中→高）

2022

- 公立学校の教師の勤務時間の上限に関するガイドライン
- 教育情報セキュリティポリシーに関するガイドライン **更新**

2024年を目標に「児童生徒1人1台PC」を実現！学校環境だけでなく教育にも広がるICT化

GIGAスクール構想による１人１台端末環境の実現等について

児童生徒１人１台コンピュータを実現することで、これまでの我が国の教育実践と最先端のICTのベストミックスを図り、教師・児童生徒の力を最大限に引き出す。災害や感染症の発生等による学校の臨時休業等の緊急時における、児童生徒の学びの保障の観点からも、ICTを効果的にフル活用することが重要である。ハード面の整備だけでなく、ソフト・指導体制を一体とした改革を強力に推進する。

<ハード>
ICT環境整備の抜本的充実

<ソフト>
デジタルならではの学びの充実

<指導体制>
日常的にICTを活用できる体制

<配備スケジュール>

2019年末	政府が事業費を計上した補正予算を決定
2020年度	小中学校に向けパソコン配備開始
2024年度	全ての配備完了

※参照：文部科学省「1人1台端末等のICT環境の活用に関する方針・チェックリストについて」https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/mext_01798.html

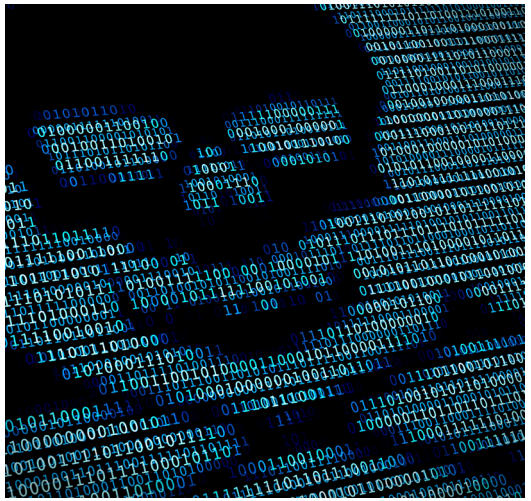
拡大するICT化により様々なリスクが発生！教育現場にも強固なセキュリティ対策が求められます

教育現場では強固な情報セキュリティの専門部隊があるわけではなく、セキュリティリテラシーにも課題あり

PC・USBメモリの盗難紛失

生徒の成績や個人情報が入った**USBメモリやPCを紛失**することで情報漏洩するケースが多発！ICT化の推進が始める以前より起こっており、非常に多いセキュリティインシデント

ウイルス感染



自宅で作業したデータを学校のPCで開いたところウイルス感染。**自宅PCがウイルス感染していたため**と考えられ、学校のセキュリティ対策だけでは防げないケース有

不正アクセス・ハッキング

教育情報システムに不正アクセスされ1万件以上の個人情報が漏洩。学校の無線LANを悪用し、違法に取得した生徒のアカウントでシステムに侵入されていた

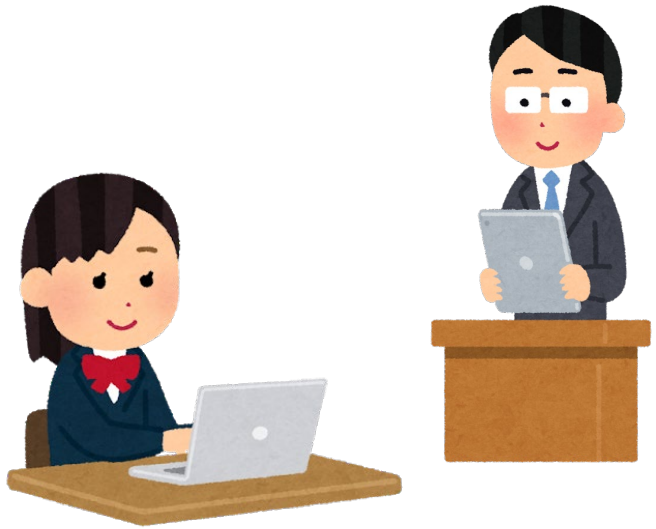
サイバー攻撃

教育委員会からのメールだったため疑いなく**添付ファイルを開きウイルス感染**。攻撃者によるなりすましだった。巧妙化するサイバー攻撃を防ぐための知識不足が原因

教育現場における情報セキュリティの策定・見直しのためのポリシーを解説するガイドラインです

今回で3回目の改版。総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」が基本方針とされています

文部科学省 MINISTRY OF EDUCATION, CULTURE, SPORTS, SCIENCE AND TECHNOLOGY-JAPAN



ガイドラインのポイント

- 教育現場の実態に合わせた情報セキュリティ対策の確立
- 児童の重要度の高い情報へのアクセスリスク対応
- 標的型攻撃などの外部脅威対策
- 教育現場の実態を踏まえた情報セキュリティ対策の確立
- 教職員の情報セキュリティ意識と醸成
- 教職員の業務負担軽減及びICTを活用した学習の実現

※参照：文部科学省「教育情報セキュリティポリシーに関するガイドライン」https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm

今回の改定では「サイバー攻撃対策」や「情報持ち出し」「公務端末の使い分け」について言及

① アクセス制御による対策の詳細な技術的対策の追記

アクセス制御による対策を講じたシステム構成を実現するために校務用端末における詳細なセキュリティ対策を追記

項目	概要
校務用端末の詳細なセキュリティ対策の追記	「リスクベース認証」※1、「ふるまい検知」※2、「マルウェア対策」、「暗号化」、「SSOの有効性」などの記述を充実

※1 リスクベース認証：システムへの接続において場所や時間などが通常と異なる場合などにID・パスワードだけではなく追加の認証を行う方式
※2 ふるまい検知　：通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み

② 「ネットワーク分離による対策」、「アクセス制御による対策」を明確に記述

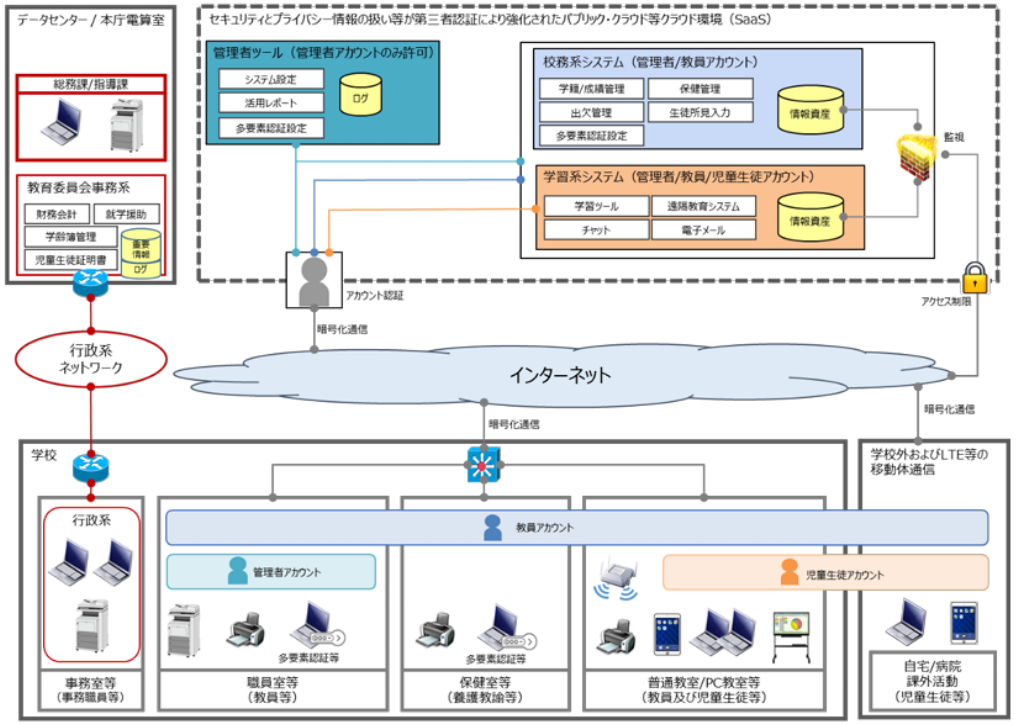
「ネットワーク分離による対策」及び「アクセス制限による対策」の記述を分岐させることにより表現を適正化

項目	概要
校務用端末の使い分けについて対策毎に記述を適正化	ネットワーク分離による対策を講じたシステム構成の場合 ・ネットワーク毎に複数の端末を使い分ける ※シンクライアント技術等を用いてネットワーク分離に準ずる対策を行い1台の端末で運用する アクセス制御による対策を講じたシステム構成の場合 ・アクセス制御を徹底することにより１台の端末で運用
校務用端末の持ち出しに関する記述を適正化	ネットワーク分離による対策を講じたシステム構成の場合 ・安全管理に関して追加的な措置を定めた上で許可制とする ※MDMによる遠隔でのデータ削除対策や、持ち出しデータを記録しておき返却時には削除するなどの追加的な措置 アクセス制御による対策を講じたシステム構成の場合 ・情報セキュリティ管理者の包括的承認等による持ち出しを検討する

※参照：教育情報セキュリティポリシーに関するガイドライン(令和4年3月)改訂説明資料 https://www.mext.go.jp/content/20220303-mxt_shuukyo01-100003157_005.pdf

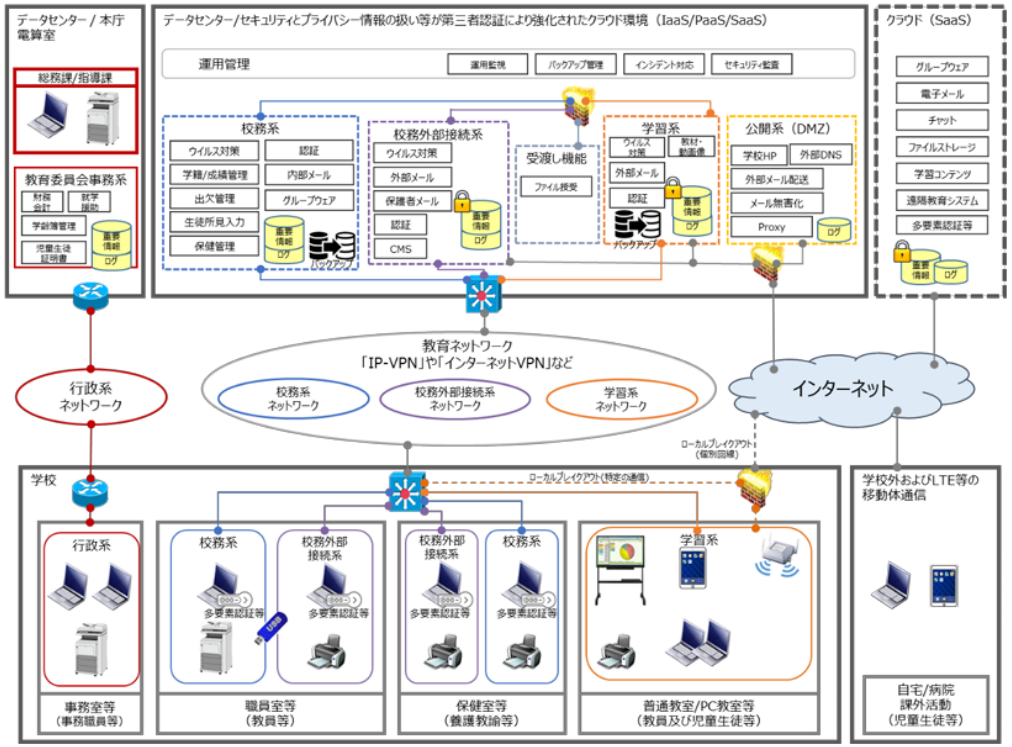
ネットワーク環境は学校毎に体制に応じて選択！採用する環境によって参照するガイドラインが異なります

●クラウドで認証によるアクセス制御を前提とした構成（※下図は学校直収型）



- 学校からの接続形態は、「センター集約型」か「学校直収型」
- クラウドサービスで管理されているデータは、サービス提供事業者により厳格管理されているものとする（そのため分離は不要）
- ネット接続があるネットワークは特にセキュリティ対策に注意

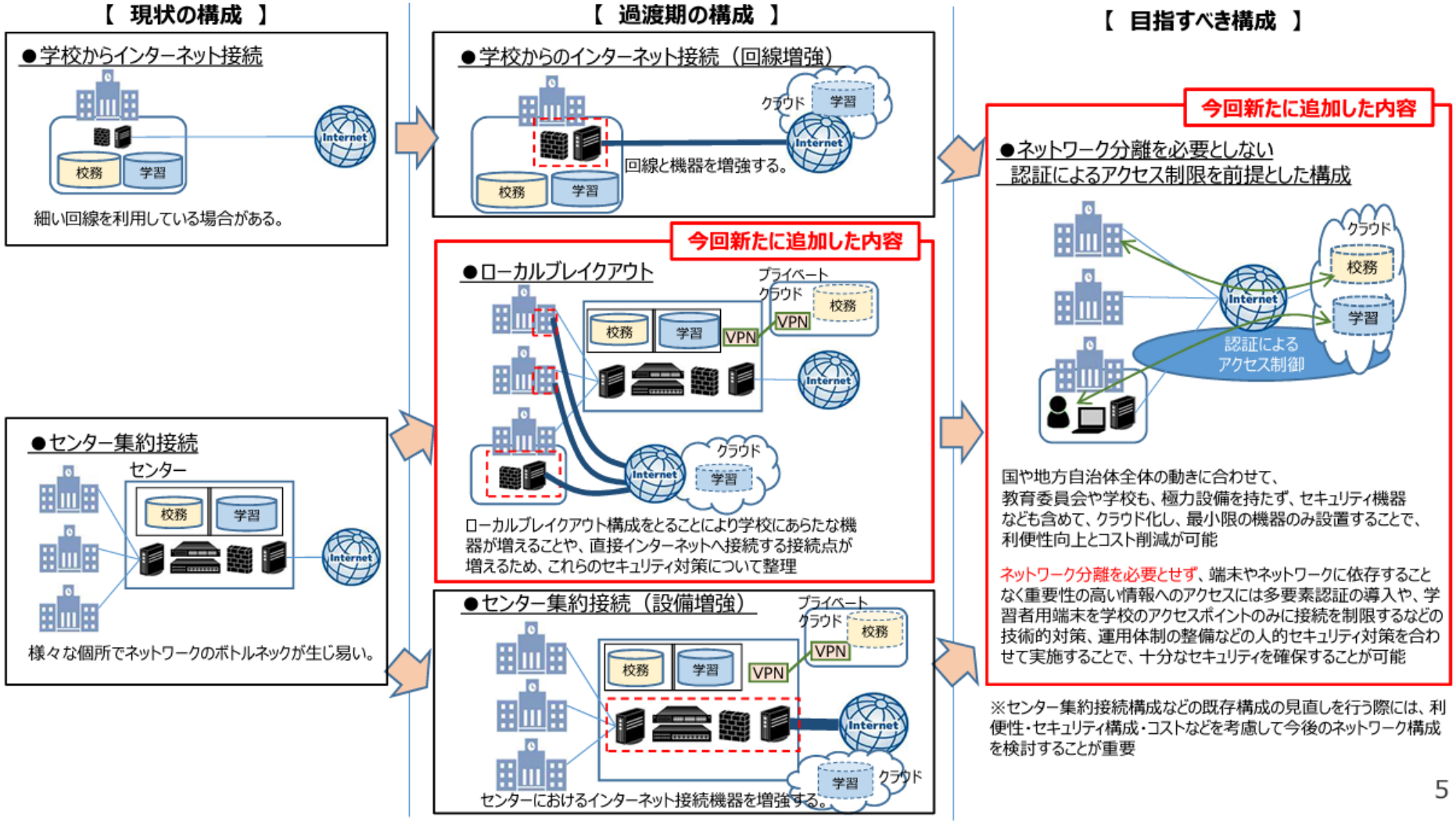
●ネットワーク分離環境構成（※下図はセンター集約型）



- 学校からの接続形態は、「センター集約型」か「学校直収型」
- ローカルブレイクアウトする場合のネットワークはセキュリティ対策を施す事。さらにIot機器の性能や状態をしっかり管理すること

※参照：文部科学省「教育情報セキュリティポリシーに関するガイドライン」https://www.mext.go.jp/content/20220304-mxt_shuukyo01-100003157_1.pdf

ネットワーク分離を必要としない認証を目指す場合、ステップを踏んで体制構築しましょう



※参照：「教育情報セキュリティポリシーガイドライン」の第２回改訂に関する説明資料　https://www.mext.go.jp/content/20210528-mxt_jogai02-000011648_001.pdf

LANSCOPE で対応する情報セキュリティポリシーガイドライン

教育情報セキュリティポリシーに関するガイドライン対応を行える３つのプロダクト

エンドポイント管理ツール

Endpoint Manager

組織の IT 資産管理・内部不正対策・外部脅威対策をオールインワンで対応可能です。オンプレミス版、クラウド版を用意し、クラウド版では PC 管理に加えてスマホ管理も支援します。

業界最高峰の AI アンチウイルス

Cyber Protection

AI を活用したアンチウイルスで、未知・亜種のマルウェアからデバイスを防御します。高性能なエンドポイントセキュリティ「CylancePROTECT」「Deep Instinct」を MOTEX が提供する安心サポートで導入できる Managed サービスです。

Microsoft 365 の情報漏洩対策

Security Auditor

Microsoft 365 の監査ログを取得・整形しレポート化。情報漏洩などのインシデントに繋がる操作を把握できます。また、様々なクラウドサービスと連携することで複雑な業務を自動化し、ユーザー自身が課題を解決できる最適なフローを提供します。

PC・スマホのリモートサポート

Remote Desktop

遠隔地にあるサーバーや PC、スマホへの「リモート操作」「画面共有」を実現する企業向けのリモートコントロールツールです。オンプレミス版、クラウド版から選択して導入できます。

コンサルティング・ソリューション導入、運用監視支援

Professional Service

サイバーセキュリティのさまざまな領域に対し、「診断・コンサルティング」「対策」「監視」という3つの観点で、リスクアセスメントを含むコンサルティング、対策導入、運用までのトータルセキュリティソリューションを提供します。

LANSCOPE で支援する「教育情報セキュリティポリシーに関するガイドライン」対策

情報セキュリティ対策基準			対応機能	対応製品
1.4 物理的セキュリティ	1.4.4　教職員等の利用する端末や電磁的記録媒体等の管理	⑦モバイル端末のセキュリティ NEW	リモートロック・ワイプ	LANSCOPE Endpoint Manager
		⑧マルウェア対策 NEW	マルウェア対策 ログ取得	LANSCOPE Cyber Protection
		⑨不適切なウェブページの閲覧防止 NEW	Webフィルタリング	LANSCOPE Endpoint Manager
1.5 人的セキュリティ	1.5.1 教職員等の遵守事項	②業務以外の目的でのインターネットへのアクセスの禁止	Webアクセス管理	
		③モバイル端末の無断持出しの禁止	モバイル管理	
		④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の利用禁止	デバイスの利用制御	
1.6 技術的セキュリティ	1.6.1 コンピュータ及びネットワークの管理	(６) ログの取得等	ログ管理・サーバー監視	
		(１８) 無許可ソフトウェアの導入等の禁止	ソフトウェアのインストール制限	
		(２０) 無許可でのネットワーク接続の禁止	不許可端末検知・遮断	
	1.6.4 不正プログラム対策	(１) 統括教育情報セキュリティ責任者の措置事項 ④コンピュータウイルス等の不正プログラム対策ソフトウェアの常駐	マルウェア対策	LANSCOPE Cyber Protection
	1.6.6 セキュリティ情報の収集	(１) セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等	ソフトウェア配布	LANSCOPE Endpoint Manager
1.7 運用	1.7.1　情報システムの監視		レポート・アラーム管理	
	1.7.2 教育情報セキュリティポシーの遵守状況確認	（１）遵守状況の確認及び対処	レポート・ログ管理	
		（２）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査	デバイスの使用制限・ログ管理	
1.9 クラウドサービスの活用	1.9.2 クラウド サービス の利用における情報セキュリティ対策		ー	

1.4.4 教職員等の利用する端末や電磁的記録媒体等の管理

⑦モバイル端末のセキュリティ

モバイル端末を学校外で業務利用する場合は、端末の紛失・盗難対策として、前述のように普段からパスワードによる端末ロックを設定しておくことが必要である。また、紛失・盗難に遭った際は、遠隔消去（リモートワイプ）や自己消去機能により、モバイル端末内のデータを消去する対策も有効である。

リモートロック・ワイプ

位置情報・移動履歴の取得が可能で
有事の際にはリモートでロックワイプ

位置情報を取得し、端末がどこにあるのかを可視化することができます。さらに移動履歴も追えるため、盗難紛失時には早急に対応を取る事が可能です。

万が一の場合は、そのまま遠隔でリモートロックワイプが迅速に行えます。

1.4.4 教職員等の利用する端末や電磁的記録媒体等の管理
⑧マルウェア対策
近年のサイバー攻撃は複雑、巧妙化しており、パターンファイルによる不正プログラム対策ソフトウェアでは検知出来ない攻撃が頻発している状況である。こうしたマルウェアを検知するためには、既存のパターンファイルから検出する手法に加え、ふるまい検知が有効である。ふるまい検知とは、既存のパターンファイル情報に依存することなく、各端末における通常時の通信傾向を学習し、そこから逸脱する不審な通信について検知する仕組み。隔離された安全な領域（サンドボックス）で不審なプログラムの挙動を検知することにより、未知の攻撃にも有効である。 なお、マルウェアに感染し攻撃を検知した場合には、その根本原因や感染した端末の特定と隔離、影響範囲の関係や時系列での不正なふるまいの状況を一元的に把握することができるEDR（Endpoint Detection and Response）も有効である。運用体制・端末のリソース状況・実現したい機能・コストを鑑みて検討すること。

マルウェア対策

マルウェア以外の脅威を未然に発見
調査・封じ込め・復旧まで一連の対応が可能

検知したマルウェア以外の「危険なプロセス」や「コマンドの実行」など「端末に潜む脅威」を発見、攻撃の流れを操作を紐づけて可視化することで、未然に脅威を察知し、対策することが可能です。

＜LANSCOPE サイバープロテクションは予防にフォーカスしたEDR機能を保有＞

攻撃防御 › 検知 › 調査 › 封じ込め › 復旧

Powered by CylancePROTECT

・オプション機能として提供（CylanceOPTICS）
・定期レポートなどサービスが充実

Powered by deepinstinct BEFORE YOU KNOW IT

・簡易的なEDR機能を標準機能として実装
・事前防御にフォーカス・根本対策のためのEDR機能

1.4.4 教職員等の利用する端末や電磁的記録媒体等の管理
⑨不適切なウェブページの閲覧防止
アクセス制御による対策を講じたシステム構成の場合、不適切なウェブページへの閲覧を防止する対策として「フィルタリングソフト」、「検索エンジンのセーフサーチ」、「セーフブラウジング」等がある。実現したい機能や実際の運用に応じて適切に整備することが重要である。

Webフィルタリング

クラウドサービスや Web メールのログを取得
リスクのあるサイトアクセスを制御できます

Web アクセスの閲覧記録、特定 Web サイトやカテゴリごとの閲覧制御ができます。ユーザーの適切な Web 利用を促進し、有害サイトへのアクセスを防ぎます。

クライアント型のため接続するネットワーク環境などに左右されず、監視や制御ができます。

●クライアント型Webフィルタリング

1.5.1 （1）教職員等の遵守事項
②業務以外の目的での使用の禁止
教職員等は、業務以外の目的で情報資産の外部への持ち出し、教育情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

Webアクセス管理

インターネットアクセス履歴をログ化し収集
カテゴリごとにフィルタリングできます

Web サイトの閲覧記録、特定Web サイトやカテゴリごとの閲覧制御ができます。ユーザーの適切なWeb 利用を促進し、有害サイトへのアクセスを防ぎます。

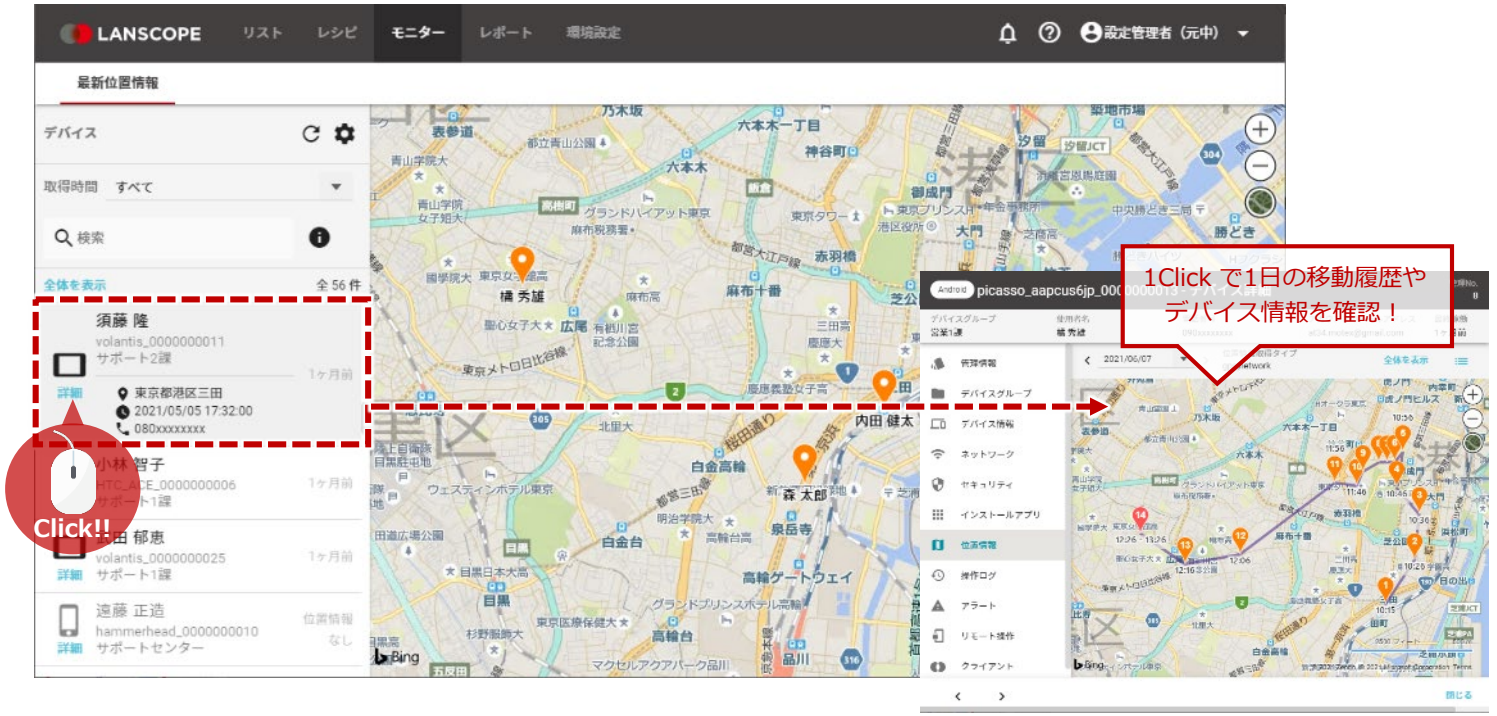
公衆ネットワークでのWeb 利用も監視や制御ができます。

1.5.1 （1）教職員等の遵守事項
③モバイル端末の無断持出しの禁止
モバイル端末や電磁的記録媒体等の持ち出し及び教育委員会・学校が構築・管理している環境(本ガイドラインが適用されているクラウドサービスや学校外での利用が認められている情報端末等を含む環境)の外部における情報処理作業の制限 (イ)教職員等は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、教育情報セキュリティ管理者の許可を得なければならない。

持ち出し対策

端末の現在地・移動履歴を把握できます

端末の現在地を確認し、不正持ち出しが無いかを確認できます。万が一の場合は、1日の移動履歴を確認し、どのくらいの間、どこに持ち出されていたかを確認できます。

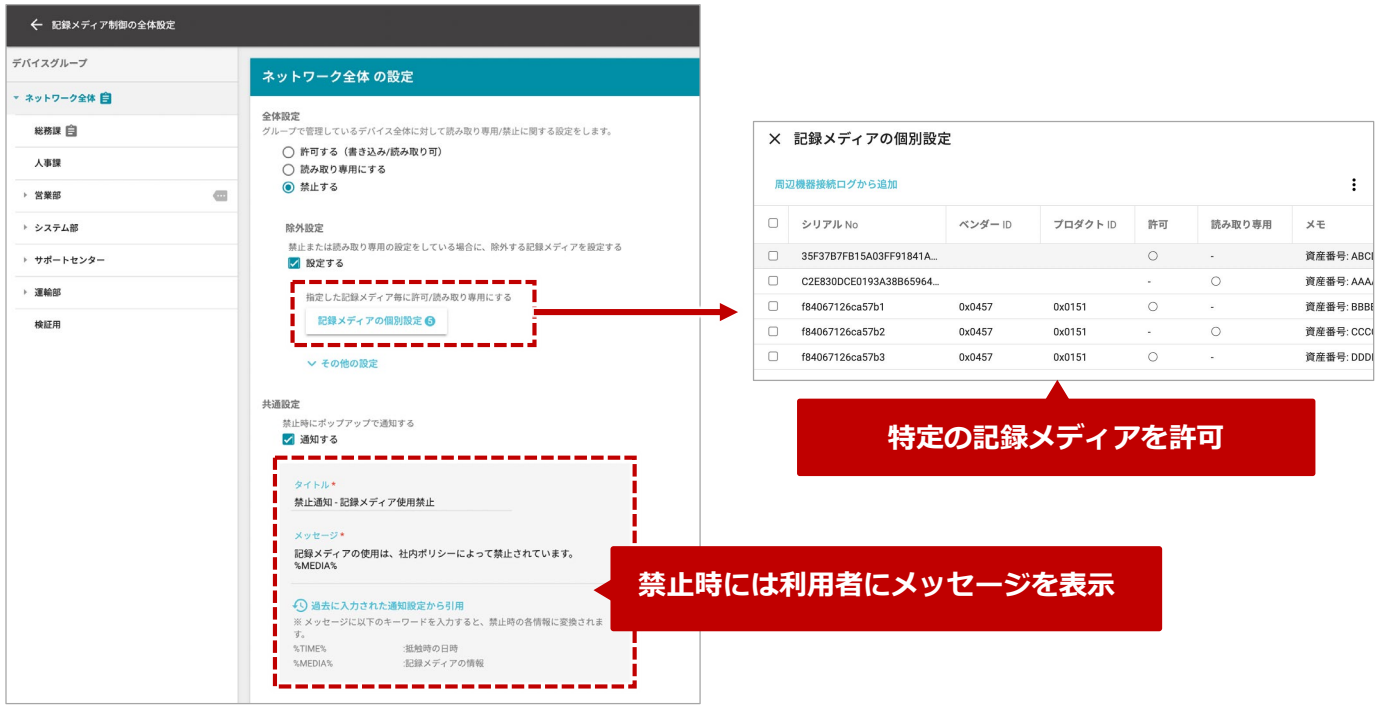


1.5.1 （1）教職員等の遵守事項
④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用
(ア)教職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、教育情報セキュリティ管理者の許可を得て利用することができる。

デバイス制御

会社支給以外の電磁的記録媒体の利用を制御（禁止）できます

社内のデバイスの一元管理・利用を制御が可能。支給禁止デバイスが接続されると、ユーザーに禁止通知し、不正利用を抑制できます。
また、PC ごとデバイスごとの詳細な条件で限定的にデバイス利用を許可し、現場に即した運用が可能です。



1.6.1. コンピュータ及びネットワークの管理

（６）ログの取得等

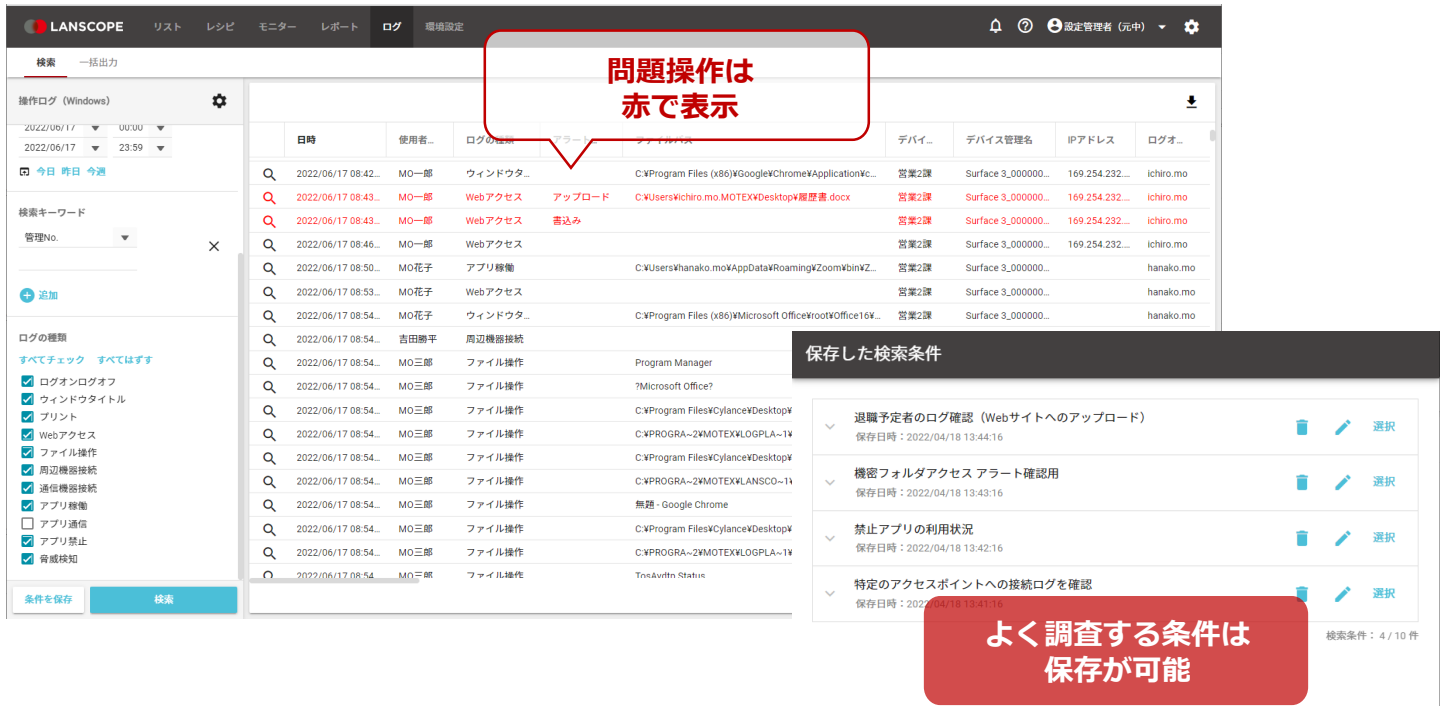
①統括教育情報セキュリティ責任者及び教育情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。
③統括教育情報セキュリティ責任者及び教育情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

ログ管理

PC 操作を記録し、問題の有無を把握。さらに問題発生時の詳細調査ができます

パソコンの操作履歴をログ化し収集可能です。問題操作が発生した場合、赤字で問題操作をお知らせします。気になる操作はクリックし周辺操作を確認できます。

「退職者の操作を把握する」などよく調査する条件は保存が可能です



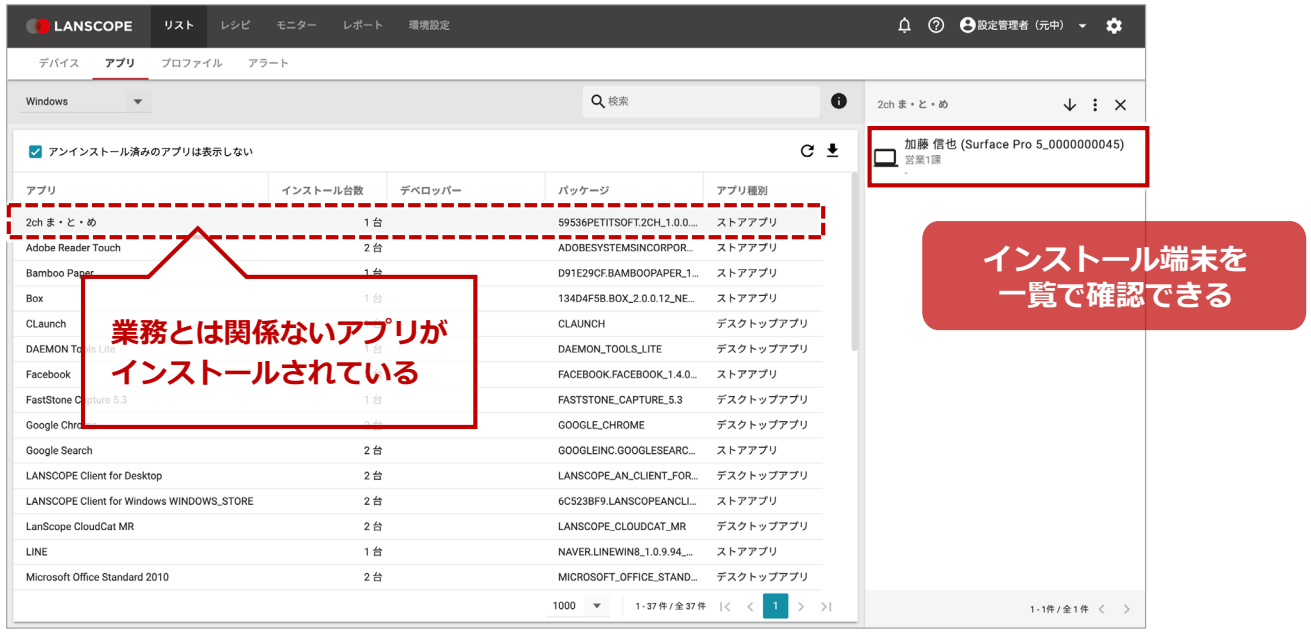
1.6.1. コンピュータ及びネットワークの管理
（１８）無許可ソフトウェアの導入等の禁止
①教職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

アプリ管理

許可なくパソコンにソフトウェアを インストールできないように禁止できます

インターネットからソフトウェアをダウンロードしてパソコンにインストールすると不正プログラムに感染するといった可能性があります。

そのため、教職員が勝手にソフトウェアをインストールできないようパソコンを制限する対策が必要です。



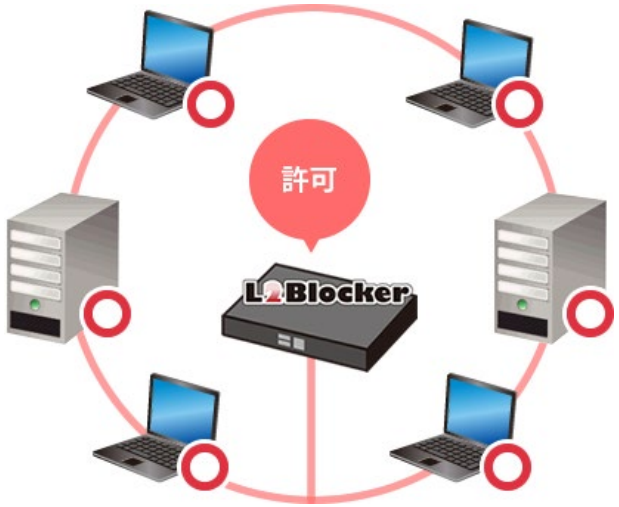
1.6.1. コンピュータ及びネットワークの管理
（２０）無許可でのネットワーク接続の禁止
教職員等は、統括教育情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

不正PC検知・遮断

私物パソコンからの校内ネットワーク接続を検知・遮断できます

セキュリティ上、ネットワークとの接続には適切な管理が必要であるため、教職員の私物パソコンなど、管理者の許可がない端末でネットワークに接続した際は管理者に通知または遮断できます。24時間365日の検知・遮断が可能のためリスクある管理者がいなくても守る事が可能です。

●管理下にある機器は自動で許可



●管理外の機器は自動で遮断

※LANSCOPE エンドポイントマネージャーでの連携製品「L2Blocker」の導入が必要です

1.6.4 不正プログラム対策
(1) 統括教育情報セキュリティ責任者の措置事項
④所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

マルウェア対策

AIを活用した新方式のためパターンファイルが不要！毎日のアップデートは不要です

AIエンジンを活用した新技術でマルウェアを検知し、端末をマルウェア感染から保護します。
これまでのウイルス対策ソフトやふるまい検知、サンドボックスのように止められないことが前提の事後対策ではなく、未知の脅威でも実行前に検知し防御することができます。

※　2018 NSS Labs Advanced Endpoint Protection Test 結果より

新方式で検知するLANSCOPE サイバープロテクションは
パターンファイル・サンドボックスなどを使わない新方式です

高い検知精度

AI（人工知能）による自動判断

DNAレベルのマルウェア解析

管理負担・端末負担を軽減

毎日のアップデートが不要

管理者や端末に負担をかけない

1.6.6 セキュリティ情報の収集
(1) セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等
統括教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

ダッシュボード

脆弱性の有無が一目で分かり その対策が簡単にできます

ダッシュボードでは、組織に存在する端末の中で、最新の状態に保たれていない脆弱な端末を自動で抽出しカードに表示します。カードの詳細には適用すべきパッチの情報を含んでいるため、専門的な知識がなくても、必要な対策を実施できます。対策情報はMOTEX から更新されるので、毎日ダッシュボードを確認するだけで、社内の脆弱な端末の発見・対策を支援します。

1.9.2 クラウド サービス の利用における情報セキュリティ対策
校務系システム、学習系システムにおいてクラウドサービスを利用する場合、クラウドの利用者である教育委員会等（以下、クラウド利用者と言う）は、クラウド事業者が、自らの情報資産を預けるに値する安心安全で信頼できるパートナーであることを慎重に確認しなければならない。

ISO27017 認証取得

LANSCOPE エンドポイントマネージャー クラウド版はクラウドセキュリティの国際規格を取得

LANSCOPE エンドポイントマネージャー クラウド版は、クラウドセキュリティの国際規格「ISO/IEC 27017」の認証を取得しています。クラウドサービスのための情報セキュリティ管理策の実践と規範がなされていることを認定する国際規格のため安心してご利用いただけます

Cloud LANSCOPE Endpoint Manager

- iOS・Android・Windows・macOSを一元管理
- Apple・Googleの認定プログラム対応で充実のモバイル管理
- 操作ログ・ファイル配信・記録メディア制御でPC管理

bsi ISMS-AC ISMS ISR004 -CLS

bsi ISO/IEC 27017 Cloud Security Management CERTIFIED

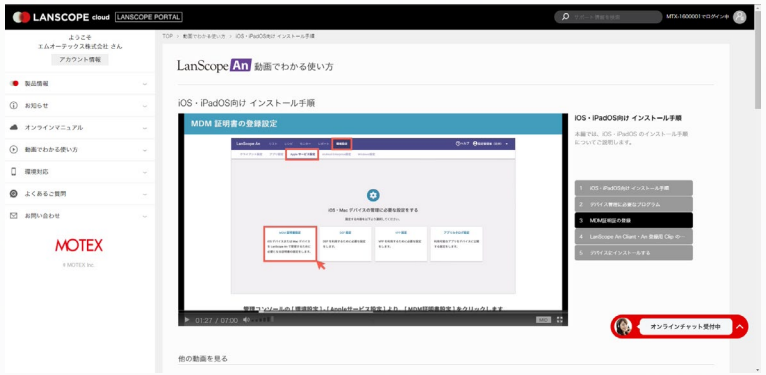
Cloud
LANSCOPE
Endpoint Manager

60日間無料体験キャンペーン中

LANSCOPE エンドポイントマネージャー クラウド版の体験版は 60日間たっぷり利用できます。十分に機能を検証していただき、ご検討ください。設定したポリシーや取得した情報を含め、そのまま製品版へのデータ引き継ぎが可能です。また体験版利用中も、弊社サポートセンターにお電話やメールで問い合わせが可能。体験期間中は、マニュアルやオンラインで学べるトレーニング動画も公開しています

●各種マニュアル・問い合わせが可能

●動画で設定方法を説明



https://go.motex.co.jp/l/320351/2017-06-21/c55z

LANSCOPE
Cyber Protection

AIアンチウイルス無料体験実施中 ― 選べる2つの検知エンジン ―

CylancePROTECT

概　　要	CylancePROTECTが**キャンペーン期間中にライセンス数無制限**で使えます。また、検知したファイルについてサマリーレポートを作成させて頂きます。さらに専任スタッフによる**導入時の支援付き**で、負担なく使い始められます。
対　　象	CylancePROTECTを初めて導入するユーザー様
ご利用期間	1ヶ月間
申　込　み	キャンペーンサイトからエントリー https://go.motex.co.jp/l/320351/2019-06-27/2fv6jr
お申込み期限	2022年9月30日

deep instinct™

概　　要	DeepInstinct が**100Lまで、1ヶ月間無料**でお試し頂けます。 さらに専任スタッフによる**導入時の支援付き**で、負担なく使い始められます。体験中の不明点にも対応しますので、じっくりしっかり体験が 可能です。
対　　象	DeepInstinctを初めて導入するユーザー様
ご利用期間	1ヶ月間
申　込　み	キャンペーンサイトからエントリー https://go.motex.co.jp/l/320351/2021-02-25/4gnpt1
お申込み期限	常時受付

本資料に関するお問い合わせ

■ マーケティング本部
プロダクトマーケティング部
E-mail　product@motex.co.jp

ご導入後の製品利用に関するお問い合わせ

サポートセンター　0120-968995 （携帯・PHSからは06-6308-8981）
お電話受付時間　9:30～12:00/13:00～17:30（平日、祝祭日除く）
Email お問い合わせ　support@motex.co.jp

本資料は2022年3月版　文部科学省「教育情報セキュリティポリシーに関するガイドライン」に基づいて作成しています。
あくまで抜粋・まとめ版となりますので、対策時には正式版もご参照いただくことを推奨します
文部科学省：https://www.mext.go.jp/content/20220304-mxt_shuukyo01-100003157_1.pdf